



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/803,772	03/17/2004	Burjiz Pithawala	50325-0829	8045
29/989 7590 03/04/2010 HICKMAN PALERMO TRUONG & BECKER, LLP 2055 GATEWAY PLACE SUITE 550 SAN JOSE, CA 95110				
EXAMINER HENRY, MARIEGEORGES A				
ART UNIT 2455		PAPER NUMBER		
MAIL DATE 03/04/2010		DELIVERY MODE PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/803,772

Applicant(s)

PITHAWALA ET AL.

Examiner

Marie Georges Henry

Art Unit

2455

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 December 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2, 34, 54 and 68-98 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 2, 34, 54, and 62-98 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB-06)
Paper No(s)/Mail Date _____

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This is in response to the communication filed on 12/15/2009. A replacement Final Action is issued replacing the previous action mailed on 06/ 23/2009. Claims 34 and 54 are amended. Claims 1, 3-33, 35-53, and 56-61 are cancelled. Claims 62-98 are new. Claims 2, 34, 54, and 62-98 are pending. Claims 2, 34, 54, and 62-98 are directed to method and apparatus providing device-initiated network management.

2. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21 (2) of such treaty in the English language.

4. Claims 34, 54, 62- 65, 67-71, 77, 83- 86, 88- 92, and 98 are rejected under 35 U.S.C. 102(b) as being anticipated by **Karjala et al.** (hereinafter "Karjala") (**US 2004/0268148 A1**).

Regarding claim 34, Karjala discloses a method comprising the computer-implemented steps of:

requesting a management gateway that is communicatively coupled to the network element to provide one or more management requests for a network element (Karjal, [0114], fig.2, a gateway is communicating with an application on device to provide updated policy); wherein the one or more management requests have been

stored at the management gateway by a management application (Karjala, [0107], EGW, enrollment gateway, uses SSM server to store certificates to authenticate requests);

in response to said requesting, receiving from the management gateway at least a particular management request (Karjala, [0114], fig.5, a request is received from SSM server, policy Management application, for an authentication based on certification);

in response to the particular management request, initiating at the network element communication of a reply to the particular management request, via the management gateway (Karjala, [0113], in response to a Web server providing HTML pages a file is downloaded);

wherein the management application is logically separate from the management gateway (Karjala, [0104], fig.2, the SSM server and Radius server are different entities); wherein the network element is an element of a device that does not execute the management application or the management gateway (Karjala, [0114], fig.2, a proxy is disclosed distinct from a SSM server and a client device); wherein the method is performed by a computing devices (Karjala, [0019], a LAN disclosed has several servers).

Regarding claim 54, Karjala discloses a computer-readable storage medium storing one or more instructions wherein the one or more instructions, when executed by one or more processors, cause:

requesting a management gateway that is communicatively coupled to the network element to provide one or more management requests for a network element (Karjala, [0114], fig.2, a gateway is communicating with an application on device to provide updated policy);

wherein the one or more management requests have been stored at the management gateway by a management application (Karjala, [0107], EGW, enrollment gateway, uses SSM server to store certificates to authenticate requests);

in response to said requesting, receiving from the management gateway at least a particular management request (Karjala, [0114], fig.5, a request is received from SSM server, policy Management application, for an authentication based on certification);

in response to the particular management request, initiating at the network element a communication of a reply to the particular management request, via the management gateway (Karjala, [0113], in response to a Web server providing HTML pages a file is downloaded);

wherein the management application is logically separate from the management gateway (Karjala, [0114], fig.2, a gateway is disclosed distinct from a SSM server and a client device); wherein the network element is an element of a device that does not execute the management application or the management gateway (Karjala, [0114], fig.2, a client device disclosed is not located in the same device than SSM server).

Regarding claim 62, Karjala discloses an apparatus comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom (Karjala, [0103], a Web server disclosed is acting as an external interface to SSM server); one or more processors (Karjala, [0019], a LAN disclosed has several servers);

one or more stored sequences of instructions which, when executed by the one or more processors, cause the one or more processors to perform:

receiving a request from a management application for interaction with the network entity (Karjala, [0115], fig.5, a request is received from SSM server, policy Management application, for a HTTP connection with a client);

based at least upon the request from the management application, creating a management request (Karjala, [0116], a certification authority to forward a certificate

request that manages the request is forwarded by EGW, enrollment gateway, over HTTP);

storing said management request at the apparatus while awaiting a poll for the management request from the network entity (Karjala, [0107], EGW, enrollment gateway, uses SSM server to store certificates to authenticate requests); receiving a poll message from the network entity, said poll message requesting from the apparatus any available management requests applicable to the network entity (Karjala, [0114], a request for a policy update comes from a client using a proxy);

in response to the poll message:

selecting one or more management requests stored in the apparatus that match the network entity; and delivering the selected one or more management requests to the network entity (Karjala, [0025], fig.9, using a selection menu, a software can be selected and installed by using a display feature having install and view certificate options); wherein the apparatus is external to the management application and the network entity (Karjala, [0114], fig.2, a proxy is disclosed distinct from a SSM server and a client device).

Regarding claim 63, Karjala disclose the apparatus as recited in Claim 62, in addition Karjala discloses the apparatus wherein the one or more stored sequences of

instructions, when executed by the one or more processors, further cause the one or more processors to perform:

receiving a responsive management message from the network entity (Karjala, [0113], a user is sending a HTTP request responding to Web server); storing the responsive management message in the apparatus (Karjala, [0107], EGW, enrollment gateway, uses SSM server to store certificates to authenticate requests);

receiving a second poll message from the management application, wherein the second poll message requests any responsive management messages applicable to the management application (Karjala, [0114], a request for a policy update comes from a client using a proxy);

in response to the second poll message:

selecting one or more responsive management messages that match the management application; and delivering the selected one or more responsive management messages to the management application (Karjala, [0025], fig.9, using a selection menu, a software can be selected and installed by using a display feature having install and view certificate options).

Regarding claim 64, Karjala disclose the apparatus as recited in Claim 62, in addition

Karjala discloses the apparatus wherein the network entity is within a private network that is managed by a network service provider, and wherein the apparatus and the management application are within a public network that is owned or operated by the network service provider (Karjala, [0020], the network system disclosed has an internet and a Intranet).

Regarding claim 65, Karjala disclose the apparatus as recited in Claim 62, in addition Karjala discloses the apparatus wherein the network entity is a service appliance (Karjala, [0023], a mobile phone is disclosed).

Regarding claim 67, Karjala disclose the apparatus as recited in Claim 62, in addition Karjala discloses the apparatus wherein the network entity is a device with which the management application is unable to directly communicate (Karjala, [0114], fig.2, a client device is accessing the Radius server by using a proxy).

Regarding claim 68, Karjala discloses an apparatus comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom (Karjala, [0103], a Web server disclosed is acting as an external interface to SSM server); one or more processors (Karjala, [0019], a LAN disclosed has several servers);

one or more stored sequences of instructions which, when executed by the one or more processors, cause the one or more processors to perform:

requesting a management gateway that is communicatively coupled to a network element to provide one or more management requests for a network element (Karjala, [0115], fig.5, a request is received from SSM server, policy Management application, for a HTTP connection with a client);

wherein the one or more management requests have been stored at the management gateway by a management application (Karjala, [0107], EGW, enrollment gateway, uses SSM server to store certificates to authenticate requests); in response to said requesting, receiving from the management gateway at least a particular management (Karjala, [0114], fig.5, a request is received from SSM server, policy Management application, for an authentication based on certification);

in response to the particular management request, initiating at the network element communication of a reply to the particular management request, via the management gateway (Karjala, [0114], a request for a policy update comes from a client using a proxy);

wherein the management application is logically separate from the management

gateway (Karjala, [0114], fig.2, a gateway is disclosed distinct from a SSM server and a client device); wherein the network element is an element of a device that does not execute the management application or the management gateway (Karjala, [0114], fig.2, a client device disclosed is not located in the same device than SSM server).

Regarding claim 69, Karjala disclose the apparatus as recited in Claim 68, in addition Karjala discloses the apparatus wherein the apparatus is a server that is logically separate from the network element and communicatively coupled to the management gateway (Karjala, [0114], fig.2, a client device is accessing the Radius server by using a proxy).

Regarding claim 70, Karjala disclose the apparatus as recited in Claim 68, in addition Karjala discloses the apparatus wherein the apparatus includes the network element (Karjala, [0023], a mobile phone is disclosed).

Regarding claim 71, Karjala and Green disclose the apparatus as recited in Claim 68, in addition Karjala discloses the apparatus wherein the one or more stored sequences of instructions, when executed by the one or more processors, further cause the one or more processors to perform initiating at the network element communication of at least some of the report information that is responsive to the particular management request (Karjal, [0112], Simple Mail Transfer Protocol is routing notification messages).

Regarding claim 77, Karjala disclose the apparatus as recited in Claim 68, in addition Karjala discloses the apparatus wherein the network element resides at a device with which the management application is unable to directly communicate (Karjala, [0114], fig.2, a client device is accessing the Radius server by using a proxy).

Regarding claim 83, Karjala discloses an apparatus comprising:

one or more processors (Karjala, [0019], a LAN disclosed has several servers); means for receiving a request from a management application for interaction with the network entity (Karjala, [0115], fig.5, a request is received from SSM server, policy Management application, for a HTTP connection with a client); means for based at least upon the request from the management application, creating a management request (Karjala, [0116], a certification authority to forward a certificate request that manages the request is forwarded by EGW, enrollment gateway, over HTTP);

means for storing said management request at the apparatus while awaiting a poll for the management request from the network entity (Karjala, [0107], EGW, enrollment gateway, uses SSM server to store certificates to authenticate requests); means for receiving a poll message from the network entity, said poll message requesting from the apparatus any available management requests applicable to the network entity (Karjala, [0114], a request for a policy update comes from a client using a proxy);

means for, in response to the poll message:

selecting one or more management requests stored in the apparatus that match the network entity; and delivering the selected one or more management requests to the network entity (Karjala, [0025], fig.9, using a selection menu, a software can be selected and installed by using a display feature having install and view certificate options); wherein the apparatus is external to the management application and the network entity (Karjala, [0114], fig.2, a proxy is disclosed distinct from a SSM server and a client device).

Regarding claim 84, Karjala disclose the apparatus as recited in Claim 83, further comprising:

means for receiving a responsive management message from the network entity (Karjala, [0113], in response to a Web server providing HTML pages a file is downloaded); means for storing the responsive management message in the apparatus (Karjala, [0107], EGW, enrollment gateway, uses SSM server to store certificates to authenticate requests); means for receiving a second poll message from the management application, wherein the second poll message requests any responsive management messages applicable to the management application (Karjala, [0114], a

request for a policy update comes from a client using a proxy);
means for, in response to the second poll message:

selecting one or more responsive management messages that match the management application; and delivering the selected one or more responsive management messages to the management application (Karjala, [0025],fig.9, using a selection menu, a software can be selected and installed by using a display feature having install and view certificate options).

Regarding claim 85, Karjala disclose the apparatus as recited in Claim 83, in addition Karjala discloses the apparatus wherein the network entity is within a private network that is managed by a network service provider, and wherein the apparatus and the management application are within a public network that is owned or operated by the network service provider (Karjala, [0020], the network system disclosed has an internet and a Intranet).

Regarding claim 86, Karjala and Green disclose the apparatus as recited in Claim 83, in addition Karjala discloses the apparatus wherein the network entity is a service appliance (Karjala, [0023], a mobile phone is disclosed).

Regarding claim 88, Karjala disclose the apparatus as recited in Claim 83, in addition Karjala discloses the apparatus wherein the network entity is a device with which the

management application is unable to directly communicate (Karjala, [0114], fig.2, a client device is accessing the Radius server by using a proxy).

Regarding claim 89, Karjala discloses an apparatus comprising:

one or more processors (Karjala, [0019], a LAN disclosed has several servers); means for requesting a management gateway that is communicatively coupled to a network element to provide one or more management requests for a network element (Karjala, [0114], fig.2, a gateway is communicating with an application on device to provide updated policy);

wherein the one or more management requests have been stored at the management gateway by a management application (Karjala, [0107], EGW, enrollment gateway, uses SSM server to store certificates to authenticate requests); means for, in response to said requesting, receiving from the management gateway at least a particular management request (Karjala, [0114], fig.5, a request is received from SSM server, policy Management application, for an authentication based on certification);

means for, in response to the particular management request, initiating at the network element communication of a reply to the particular management request (Karjala, [0113], in response to a Web server providing HTML pages a file is downloaded), via the management gateway; wherein the management application is

logically separate from the management gateway (Karjala, [0104], fig.2, the SSM server and Radius server are different entities);

wherein the network element is an element of a device that does not execute the management application or the management gateway (Karjala, [0114], fig.2, a proxy is disclosed distinct from a SSM server and a client device).

Regarding claim 90, Karjala discloses the apparatus as recited in Claim 89, in addition Karjala discloses the apparatus wherein the apparatus is a server that is logically separate from the network element and communicatively coupled to the management gateway (Karjala, [0114], fig.2, a gateway is disclosed distinct from a SSM server and a client device).

Regarding claim 91, Karjala discloses the apparatus as recited in Claim 89, in addition Karjala discloses the apparatus wherein the apparatus includes the network element (Karjala, [0023], a mobile phone is disclosed).

Regarding claim 92, Karjala disclose the apparatus as recited in Claim 89, in addition Karjala discloses the apparatus further comprising: means for initiating at the network element communication of at least some of the report information that is responsive to the particular management request (Karjala, [0112], Simple Mail Transfer Protocol is

Art Unit: 2455

routing messages).

Regarding claim 98, Karjala disclose the apparatus as recited in Claim 89, wherein the network element resides at a device with which the management application is unable to directly communicate (Karjala, [0114], fig.2, a client device is accessing the Radius server by using a proxy).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 72 and 93 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Karjala in view of **Green** et al. (hereinafter "Green") (**US 6, 058, 420**).

Regarding claim 72, Karjala disclose the apparatus as recited in Claim 68, in addition Karjala discloses the system wherein: the one or more stored sequences of instructions, when executed by the one or more processors, and in response thereto, initiating at the network element communication of at least some of the report information (Karjal, [0112], Simple Mail Transfer Protocol is routing notification messages).

Although Karjala discloses a request management feature with policy enforcement, he does not disclose the particular management request comprises a first definition of one or more triggers; each comprising one or more conditions, and a second definition of report information; and further cause the one or more processors to perform: determining that a particular trigger of the one or more triggers is satisfied.

Green discloses the particular management request comprises a first definition of one or more triggers (Green, column 8, lines 14-24, fig.3b, in a proxy device, data conformed with predefined conditions is monitored by a connection manager),

each comprising one or more conditions, and a second definition of report information (Green, column 3, lines 29-33, column 3, lines 35-43, the poller checks continuously network interface by sending out poller query message, when a message is polled, the proxy sends another message to the server stating an interface is

reachable); and

further cause the one or more processors to perform:

determining that a particular trigger of the one or more triggers is satisfied (Green, column 3, lines 29-33, column 3, lines 35-43, the poller checks continuously network interface by sending out poller query message, when a message is polled, the proxy sends another message to the server stating an interface is reachable).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Green network security feature in Karjala system in order to create a request management system with a network security feature in order to control attempt to establish contact with network entities (Green, abstract).

Regarding claim 93, Karjala discloses the apparatus as recited in Claim 89, in addition Karjala discloses the apparatus wherein: and in response thereto, initiating at the network element communication of at least some of the report information (Karjala, [0112], Simple Mail Transfer Protocol is routing messages).

Although Karjala discloses a request management feature with policy enforcement, he does not disclose the particular management request comprises a first definition of one or more triggers; each comprising one or more conditions and a second

definition of report information; and the apparatus further comprises: means for determining that a particular trigger of the one or more triggers is satisfied.

Green discloses the particular management request comprises a first definition of one or more triggers (Green, column 8, lines 14-24, fig.3b, in a proxy device, data conformed with predefined conditions is monitored by a connection manager),

each comprising one or more conditions, and a second definition of report information; and the apparatus further comprises: means for determining that a particular trigger of the one or more triggers is satisfied (Green, column 3, lines 29-33, column 3, lines 35-43, the poller checks continuously network interface by sending out poller query message, when a message is polled, the proxy sends another message to the server stating an interface is reachable).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Green network security feature in Karjala system in order to create a request management system with a network security feature in order to control attempt to establish contact with network entities (Green, abstract).

7. Claims 66, 78-82, and 87 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Karjala** in view of **Davies (US 6, 058, 420)**.

Regarding claim 66, Karjala disclose the apparatus as recited in Claim 62.

Although Karjala discloses a request management feature with policy enforcement, he does not disclose the apparatus wherein the network entity is a switch or router.

Davies discloses the apparatus wherein the network entity is a switch or router (Davies, column 15, lines 32-33, a router is disclosed).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Davies router in Karjala system in order to create a request management system with a network security feature in order to control attempt to establish contact with network entities.

Regarding claim 78, Karjala discloses an apparatus comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom (Karjala, [0103], a Web server disclosed is acting as an external interface to SSM server); one or more processors (Karjala, [0019], a LAN disclosed has several servers);

one or more stored sequences of instructions which, when executed by the one or more processors, cause the one or more processors to perform:

receiving one or more poll messages from one or more subscribing management applications; and in response to the one or more poll messages (Karjala, [0115], fig.5, a request is received from SSM server, policy Management application, for a HTTP connection with a client); wherein the apparatus is logically separate from the management application and the network entity (Karjala, [0114], fig.2, a device is disclosed distinct from a SSM server).

Although Karjala discloses a request management system, he does not disclose the system relaying the one or more event notifications to the subscribing management applications; receiving event notifications from one or more network entities; storing said event notifications at the apparatus.

Davies discloses the system relaying the one or more event notifications to the subscribing management applications; receiving event notifications from one or more network entities; storing said event notifications at the apparatus (Davies, column 4, lines 5-9, a server having storage capacity is receiving alarm information from the client module).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Davies alarm feature in Karjala system in order to create a request management system with a alarm feature in order to notify a selected device among devices in a network when to send a message to the management system. (Davies, column 3, lines 44-51).

Regarding claim 79, Karjala and Davies disclose the apparatus as recited in Claim 78. Although Karjala discloses a request management system, he does not disclose the system wherein the event notifications were not solicited by the management application or the apparatus.

Davies discloses the system wherein the event notifications were not solicited by the management application or the apparatus (Davies, column 4, lines 5-9, a server having storage capacity is receiving alarm information from the client module).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Davies alarm feature in Karjala system in order to create a request management system with a alarm feature in order to notify a selected device among devices in a network when to send a message to the management system (Davies, column 3, lines 44-51).

Regarding claim 80, Karjala and Davies disclose the apparatus as recited in Claim 78, in addition Karjala discloses the apparatus wherein the network entity is within a private network that is managed by a network service provider, and wherein the apparatus and the management application are within a public network that is owned or operated by the network service provider (Karjala, [0020], the network system disclosed has an internet and a Intranet).

Regarding claim 81, Karjala and Davies disclose the apparatus as recited in Claim 78.

Although Karjala discloses a request management system, he does not disclose the system in addition Karjala discloses the apparatus wherein the network entity is one of a service appliance, a switch, or a router.

Davies discloses the system wherein the network entity is one of a service appliance, a switch, or a router (Davies, column 15, lines 32-33, a router is disclosed).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Davies router in Karjala system in order to create a request management system with a network security feature in order to control attempt to establish contact with network entities.

Regarding claim 82, Karjala and Davies discloses the apparatus as recited in Claim 78, in addition Karjala discloses the apparatus wherein the network element resides at a device with which the management application is unable to directly communicate (Karjala, [0114], fig.2, a client device is accessing the Radius server by using a proxy).

Regarding claim 87, Karjala discloses the apparatus as recited in Claim 83.

Although Karjala discloses a request management system, he does not disclose the system in addition Karjala discloses the apparatus wherein the network entity is a switch or router.

Davies discloses the apparatus wherein the network entity is a switch or router (Davies, column 15, lines 32-33, a router is disclosed).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Davies router in Karjala system in order to create a request management system with a network security feature in order to control attempt to establish contact with network entities.

8. Claims 73-76 and 94-97 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Karjala**, in view of **Green**, and further in view of **Davies** (US 6, 058, 420).

Regarding claim 73, Karjala and Green disclose the apparatus as recited in Claim 72.

Although Karjala and Green disclose a request management system, they do not disclose the system wherein each of the conditions comprises an event, alarm, combination of events or alarms, or pattern of events or alarms.

Davies discloses the system wherein each of the conditions comprises an event, alarm, combination of events or alarms, or pattern of events or alarms (Davies, column 4, lines 35-43, a server receives alarm information).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Green proxy feature and Davies alarm feature into Karjala system in order to create a request management system with a proxy feature and an alarm feature in order to control attempt to establish contact with network entities (Green, abstract) and to notify a selected device among devices in a network when to send a message to the management system. (Davies, column 3, lines 44-51).

Regarding claim 74, Karjala and Green disclose the apparatus as recited in Claim 72.

Although Karjala and Green disclose a request management system, they do

not disclose the system wherein each of the conditions comprises a state of the network element.

Davies discloses the system wherein each of the conditions comprises a state of the network element (Davies, column 4, lines 47-51, a device address is part of sent information).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Green proxy feature and Davies alarm feature into Karjala system in order to create a request management system with a proxy feature and an alarm feature in order to control attempt to establish contact with network entities (Green, abstract) and to notify a selected device among devices in a network when to send a message to the management system. (Davies, column 3, lines 44-51).

Regarding claim 75, Karjala and Green disclose a method as recited in Claim 72.

Although Karjala and Green disclose a request management method, they do not disclose the method wherein the report information describes any of the triggers that were determined as satisfied.

Davies discloses the method wherein the report information describes any of

the triggers that were determined as satisfied (Davies, column 3, lines 40-42, the message indicates that the device is reachable).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Green proxy feature and Davies alarm feature into Karjala method in order to create a request management method with a proxy feature and an alarm feature in order to control attempt to establish contact with network entities (Green, abstract) and to notify a selected device among devices in a network when to send a message to the management system. (Davies, column 3, lines 44-51).

Regarding claim 76, Karjala and Green disclose the apparatus as recited in Claim 72.

Although Karjala and Green disclose a request management system, they do not disclose the system wherein the report information comprises any of a core dump from the network element, a configuration of the network element, state information for the network element, or a log of the network element.

Davies discloses the system wherein the report information comprises any of a core dump from the network element, a configuration of the network element, state information for the network element, or a log of the network element (Davies, column 3, lines 40-42, the message indicates that the address of the device that is reachable).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Green proxy feature and Davies alarm feature into Karjala system in order to create a request management system with a proxy feature and an alarm feature in order to control attempt to establish contact with network entities (Green, abstract) and to notify a selected device among devices in a network when to send a message to the management system. (Davies, column 3, lines 44-51).

Regarding claim 94, Karjala and Green disclose the apparatus as recited in Claim 93.

Although Karjala and Green disclose a request management system, they do not disclose the system wherein each of the conditions comprises an event, alarm, combination of events or alarms, or pattern of events or alarms.

Davies discloses the system wherein each of the conditions comprises an event, alarm, combination of events or alarms, or pattern of events or alarms (Davies, column 4, lines 35-43, a server receives alarm information).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Green proxy feature and Davies alarm feature into Karjala system in order to create a request management system with a

proxy feature and an alarm feature in order to control attempt to establish contact with network entities (Green, abstract) and to notify a selected device among devices in a network when to send a message to the management system (Davies, column 3, lines 44-51).

Regarding claim 95, Karjala and Green disclose the apparatus as recited in Claim 93.

Although Karjala and Green disclose a request management system, they do not disclose the system wherein each of the conditions comprises a state of the network element.

Davies discloses the system wherein each of the conditions comprises a state of the network element (Davies, column 4, lines 47-51, a device address is part of sent information).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Green proxy feature and Davies alarm feature into Karjala system in order to create a request management system with a proxy feature and an alarm feature in order to control attempt to establish contact with network entities (Green, abstract) and to notify a selected device among devices in a network when to send a message to the management system. (Davies, column 3, lines

44-51).

Regarding claim 96, Karjala and Green disclose a method as recited in Claim 93.

Although Karjala and Green disclose a request management method, they do not disclose the method wherein the report information describes any of the triggers that were determined as satisfied.

Davies discloses the method wherein the report information describes any of the triggers that were determined as satisfied (Davies, column 3, lines 40-42, the message indicates that the device is reachable).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Green proxy feature and Davies alarm feature into Karjala method in order to create a request management method with a proxy feature and an alarm feature in order to control attempt to establish contact with network entities (Green, abstract) and to notify a selected device among devices in a network when to send a message to the management system. (Davies, column 3, lines 44-51).

Regarding claim 97, Karjala and Green disclose the apparatus as recited in Claim 93.

Although Karjala and Green disclose a request management system, he does not the system wherein the report information comprises any of a core dump from the network element, a configuration of the network element, state information for the network element, or a log of the network element.

Davies discloses the system wherein the report information comprises any of a core dump from the network element, a configuration of the network element, state information for the network element, or a log of the network element (Davies, column 3, lines 40-42, the message indicates that the address of the device that is reachable).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Green proxy feature and Davies alarm feature into Karjala system in order to create a request management system with a proxy feature and an alarm feature in order to control attempt to establish contact with network entities (Green, abstract) and to notify a selected device among devices in a network when to send a message to the management system. (Davies, column 3, lines 44-51).

9. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Green**, in view of **Lavian** et al. (hereinafter "Lavian") (**US 7, 433, 941 B1**), and further in view of Davies (**US 6,058,420**).

Green discloses the invention substantially as claimed including method and apparatus providing device-initiated network management.

Regarding claim 2, Green discloses a method of managing a network entity that is initiated by the network entity, the method comprising:

performing, at a management proxy, the computer-implemented steps of:
receiving a request from a management application for interaction with the network entity; where the management proxy is external to the management application and the network entity (Green, column 10, lines 8-9, fig. 2, the Sidewinder, a software network management, sends a request and passes the calling information to the proxy; the proxy is exterior to the network device);

in response to the poll message:

Although Green discloses a request management method, he does not disclose a method selecting one or more management requests that match the network entity; and delivering the selected one or more management requests to the network entity; wherein the management proxy is external to the management application and the network entity; storing a management request in the management proxy while awaiting a poll for the management request from the network entity; receiving a poll message from the network entity, wherein the each poll message requests any

available management requests applicable to the network entity.

Davies discloses a method storing a management request in the management proxy while awaiting a poll for the management request from the network entity (Davies, column 10, lines 61-66, the connection request is stored until the poller sends a Get request command);

receiving a poll message from the network entity, (Davies, column 11, lines 16-30, the poll Request gets a response by an interface that receives that message); and delivering the selected one or more management requests to the network entity; wherein the management proxy is external to the management application and the network entity (Davies, column 3, lines 35-43, after a query message is polled, a response message is sent to the server stating an interface is reachable).

Although Green and Davies disclose a request management with a poll system, they do not disclose a method based at least upon the request from the management application, creating a management request, said poll message requesting from the management proxy any available management requests applicable to the network entity, selecting one or more management requests stored in the management proxy that match the network entity.

Lavian disclosed a method based at least upon the request from the management application, creating a management request, selecting one or more management requests stored in the management that match the network entity (Lavian, column 6, lines 26-32, column 5, lines 31-33, column 4, lines 14-15, column 8, lines 32-36, a network management application having a storage system submits requests to loopback address of an identified network device).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Davies poll feature and Lavian management entity request feature in Green method in order to create a request management method with a poll feature and an a management entity request feature in order to notify a selected device among devices in a network when to send a message to the management system (Davies, column 3, lines 44-51) and increase management capability (Lavian, column 3, lines 23-24).

Response to Argument

10. Applicant's arguments filed on June 23, 2009 with respect to claims 34, 54, and 62-98 have been considered and the rejections have been considered but are moot in view of the new ground(s) of rejection.

11. **A. The Applicant argues** Green does not teach the method “wherein the management proxy is external to the management application and the network entity.” (Remark, page 16, lines 29-32)

The Examiner disagrees because Green discloses a Sidewinder, a software network management, sends a request and passes the calling information to the proxy; the proxy is exterior to the network device. (Green, column 10, lines 8-9, fig. 2)

B. The Applicant argues that Davies does not teach “receiving a poll message from the network entity, said poll message requesting from the management proxy any available management requests applicable to the network entity.” (Remark, page 17, lines 20-24)

The Examiner disagrees Although Green discloses a request management method, he does not disclose a method selecting one or more management requests that match the network entity; and delivering the selected one or more management requests to the network entity; wherein the management proxy is external to the management application and the network entity; storing a management request in the management proxy while awaiting a poll for the management request from the network entity; receiving a poll message from the network entity, wherein the each poll message requests any available management requests applicable to the network entity.

Davies discloses a method storing a management request in the management proxy while awaiting a poll for the management request from the network entity (Davies, column 10, lines 61-66, the connection request is stored until the poller sends a Get request command);

receiving a poll message from the network entity, (Davies, column 11, lines 16-30, the poll Request gets a response by an interface that receives that message); and delivering the selected one or more management requests to the network entity; wherein the management proxy is external to the management application and the network entity (Davies, column 3, lines 35-43, after a query message is polled, a response message is sent to the server stating an interface is reachable).

Although Green and Davies disclose a request management with a poll system, they do not disclose a method based at least upon the request from the management application, creating a management request, said poll message requesting from the management proxy any available management requests applicable to the network entity, selecting one or more management requests stored in the management proxy that match the network entity.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement Davies poll feature in Green method in order to create a request management method with a poll feature in order to notify a

selected device among several devices in a network when to send a message to the management system (Davies, column 3, lines 44-51).

C. The Applicant argues that “the combination of Green, Davies, and Lavian fails to provide the complete subject matter recited in independent Claim 2.” (Remark, page 18, lines 30-32)

The Examiner disagrees, in response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Green discloses a management request method, Davies discloses a poll feature, and Lavian discloses an entity request feature.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication from the examiner should be directed to Marie Georges Henry whose telephone number is (571) 270-3226. The examiner can normally be reached on Monday to Friday 7:30am - 4:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571) 272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see

Art Unit: 2455

<http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Marie Georges Henry/

Examiner, Art Unit 2455

/saleh najjar/

Supervisory Patent Examiner, Art Unit 2455